CLAIMS

1. A method of detecting and preventing illegitimate use of certain network protocols without hindering legitimate use thereof, the method being characterized in that for an incoming stream of data packets, it consists in applying a delay function f() to each packet, thereby applying a delay that is not sufficient to hinder legitimate use, but that is sufficient to hinder illegitimate use.

2. A method according to claim 1, in particular in a signaling protocol, the method being characterized in that it consists in selecting a delay function that increases with the bit rate of the monitored stream, such that if the illegitimate use of the protocol for transporting private data exceeds a standard rate, the delay increases indefinitely, thereby practically blocking the channel that is being used illegitimately, without hindering other streams.

3. A method according to either preceding claim, characterized in that on detecting (21) the arrival of a data packet, it consists in determining (22) whether it belongs to a monitored stream, and if not, in allocating a count (CPT) thereto.

4. A method according to claim 3, characterized in that after detecting (21) the arrival of a data packet, it consists in incrementing (25), by a predetermined step, the count (CPT_N) associated with the monitored stream, and in applying the current value of the count as the argument of the delay function prior to releasing the data packet in an outgoing stream.

5. A method according to claim 4, characterized in that it consists in selecting a delay function having a positive second derivative.

6. A method according to claim 5, characterized in that the delay function is an exponential depending on the count associated with the monitored stream in application of a relationship having the form:

$$f(CPT_N) = \exp(\alpha * CPT_N + \beta), \text{ where } \alpha \geq 0.$$

7. A method according to any one of claims 3 to 6, characterized in that it consists in determining for the monitored stream a maximum permissible bit rate $CPTMAX_N$, and then in determining whether the number of packets waiting to be sent exceeds the value $CPTMAX_N$, and if so, destroying the waiting packets.

8. A method according to any preceding claim, characterized in that, for a DNS system, it consists in adapting automatically:

· in normal operation: the user is not ill-intentioned and is making use of the system as intended, the associated count CPT retaining a value close to 0;

· in abnormal operation: the user is ill-intentioned and is probably attempting to attack the system, the delay applied to the DNS packets increasing and the associated count CPT increasing; or

· in subnormal operation: the user is not ill-intentioned but is momentarily using the system beyond the intended limits, the count CPT remaining at moderate levels.

9. A method according to any one of claims 1 to 7, characterized in that it is implemented in a proxy-RADIUS server, local to the GSM network to be protected, and in that it consists in determining fields used for the control mechanism contained in the data of the EAP-SIM authentication mechanism, and then in executing the control mechanism to limit the number of authentication requests by analyzing authentication transport behavior.

10. A protocol according to any one of claims 3 to 9, characterized in that it also includes a step of detecting that the bit rate associated with a monitored stream is varying in a manner that is characteristic of illegitimate use, and of producing an alarm in the event of such illegitimate use.